PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-143359
(43)Date of publication of application : 28.05.1999

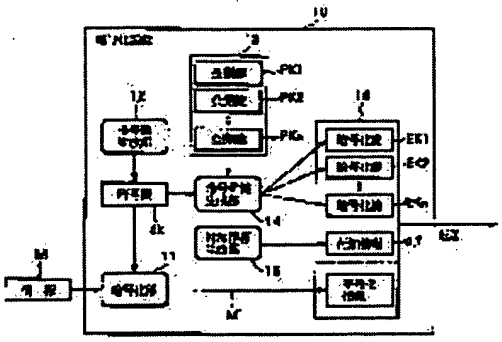
(51)Int.Cl. G09C 1/00
H04L 9/08

(21)Application number : 09-308679
(22)Date of filing : 11.11.1997

(71)Applicant : MITSUBISHI MATERIALS CORP
(72)Inventor : OOKUBO TATSUMASA
TOYODA SHOICHI

(54) ENCIPHERING DEVICE, DECODING DEVICE, INFORMATION SHARING DEVICE, ENCIPHERING METHOD, DECODING METHOD, INFORMATION PROCESSING METHOD, AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable sharing secret information by plural users by coding a code key used for enciphering with an open key of at least one user with which information can be seen, and generating plural enciphering keys.
SOLUTION: An enciphering section 11 codes input information M using an enciphering key dk for enciphering information, for example, by a sharing key cipher system, generates enciphering information M', and outputs it to a transfer section 16. A cipher key generating section 12 is constituted with random numbers generating circuit and the like, generates a coding key dk for enciphering information, and outputs it to the coding section 11 and an enciphering key generating section 14. And, the coding key generating section 14 enciphers information M using an open key of a user recorded in a storage section 13 based on an open key cipher system, generates plural enciphering keys EK1, EK2,...EKn, and outputs generated plural enciphering keys EK1-EKn to the transfer section 16.



LEGAL STATUS

[Date of request for examination] 31.03.2000
[Date of sending the examiner's decision of rejection] 30.03.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－143359

(43)公開日　平成11年(1999)５月28日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６３０	Ｇ０９Ｃ	1/00	６３０Ｄ
					６３０Ｅ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｅ
					６０１Ｄ

審査請求　未請求　請求項の数51　ＯＬ　（全 16 頁）

(21)出願番号　特願平9－308679

(22)出願日　平成９年(1997)11月11日

(71)出願人　000006264
三菱マテリアル株式会社
東京都千代田区大手町１丁目５番１号

(72)発明者　大久保　達真
埼玉県大宮市北袋町１丁目297番地　三菱マテリアル株式会社総合研究所内

(72)発明者　豊田　祥一
埼玉県大宮市北袋町１丁目297番地　三菱マテリアル株式会社総合研究所内

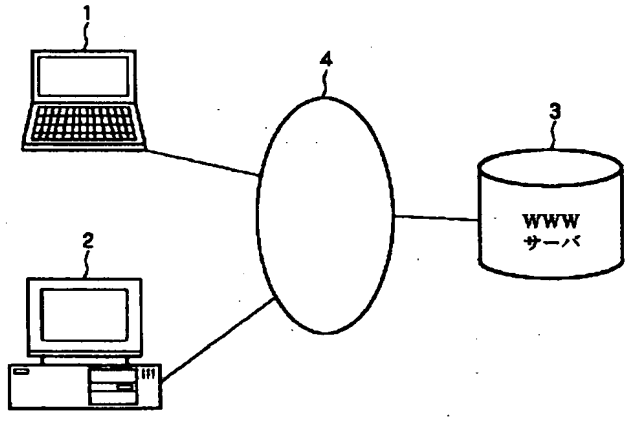
(74)代理人　弁理士　佐藤　隆久

(54)【発明の名称】　暗号化装置、復号化装置、および情報共有システム、並びに、暗号化方法、復号化方法、情報処理方法、並びに記録媒体

(57)【要約】

【課題】秘匿情報の複数ユーザによる共有が可能で、情報の内容の漏洩を防止できる暗号化装置、復号化装置を備えた情報共有システム等を提供する。

【解決手段】サーバ３と、暗号化情報を生成する暗号化部１１と、暗号鍵をユーザの公開鍵で暗号化し複数の暗号化鍵を生成する暗号化鍵生成部１４と、複数の暗号化鍵がどのユーザの公開鍵で暗号化されたものかを特定する付加情報を生成する付加情報生成部１５と、複数の暗号化鍵、暗号化情報および付加情報をサーバ３に保管させる転送部１６とを有する暗号化装置１０と、保管された複数の暗号化鍵を取得してユーザの秘密鍵で暗号化鍵を復号して暗号鍵を取得する暗号化鍵復号化部２１と、付加情報を取得して複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択部２２と、この暗号鍵に基づき暗号化情報を復号して元の情報を取得する情報復号化部２３とを有する復号化装置２０とを設ける。



1

【特許請求の範囲】

【請求項１】　情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、

暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段とを有する暗号化装置。

【請求項２】　上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段を有する暗号化装置。

【請求項３】　上記付加情報は、暗号鍵のメッセージダイジェストである請求項２記載の暗号化装置。

【請求項４】　上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ＩＤ、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項２記載の暗号化装置。

【請求項５】　上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項２、３または４記載の暗号化装置。

【請求項６】　上記複数の暗号化鍵および暗号化情報を転送する転送手段を有する請求項１記載の暗号化装置。

【請求項７】　上記複数の暗号化鍵、暗号化情報、および付加情報を転送する転送手段を有する請求項２、３、４または５記載の暗号化装置。

【請求項８】　上記転送手段は、情報を複数のユーザでアクセス可能な情報保管手段に転送する請求項６または７記載の暗号化装置。

【請求項９】　複数の暗号化鍵および暗号化情報を受けて元の情報を復号する復号化装置であって、

上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、

上記暗号鍵取得手段で取得された所定の暗号鍵に基づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置。

【請求項１０】　複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化装置であって、

上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する暗号鍵取得手段と、

上記付加情報に基づいて上記暗号鍵取得手段で取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、

上記暗号鍵選択手段で選択された暗号鍵に基づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置。

【請求項１１】　複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化

2

されたものであるかを特定する付加情報を受けて元の情報を復号する復号化装置であって、

上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、

上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、

上記暗号鍵取得手段で取得された暗号鍵に基づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置。

【請求項１２】　上記付加情報は、暗号鍵のメッセージダイジェストである請求項１０または１１記載の復号化装置。

【請求項１３】　上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ＩＤ、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項１０または１１記載の復号化装置。

【請求項１４】　上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項１０、１１、１２または１３記載の復号化装置。

【請求項１５】　取得した暗号化に利用したアルゴリズムを特定する情報をもとに、復号化のアルゴリズムを特定する手段を有する請求項１４記載の復号化装置。

【請求項１６】　複数のユーザでアクセス可能な情報保管装置と、

情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、

上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えた情報共有システム。

【請求項１７】　複数のユーザでアクセス可能な情報保管装置と、

情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、およ

び付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、
上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記情報保管装置に保管されている付加情報を取得して当該付加情報に基づき上記暗号鍵取得手段で取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えた情報共有システム。

【請求項１８】　複数のユーザでアクセス可能な情報保管装置と、
情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、
上記情報保管装置に保管されている上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号鍵に基づき上記情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えた情報共有システム。

【請求項１９】　上記付加情報は、暗号鍵のメッセージダイジェストである請求項１７または１８記載の情報共有システム。

【請求項２０】　上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ＩＤ、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項１７または１８記載の情報共有システム。

【請求項２１】　上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項１７、１８、１９または２０記載の情報共有システム。

【請求項２２】　取得した暗号化に利用したアルゴリズムを特定する情報をもとに、復号化のアルゴリズムを特定する手段を有する請求項２１記載の情報共有システム。

【請求項２３】　複数のユーザでアクセス可能な情報保管装置と、
情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置にうち、少なくとも暗号化装置を備えた第１の装置と、
上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第２の装置とを有する情報共有システム。

【請求項２４】　複数のユーザでアクセス可能な情報保管装置と、
情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記情報保管装置に保管されている付加情報を取得して当該付加情報に基づき上記暗号鍵取得手段で取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置のうち、少なくとも暗号化装置を備えた第１の装置と、
上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第２の装置とを有する情報共有システム。

【請求項２５】　複数のユーザでアクセス可能な情報保管装置と、
情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用

いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号鍵に基づき上記情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置のうち、少なくとも暗号化装置を備えた第１の装置と、

上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第２の装置とを有する情報共有システム。

【請求項２６】　上記付加情報は、暗号鍵のメッセージダイジェストである請求項２４または２５記載の情報共有システム。

【請求項２７】　上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ＩＤ、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項２４または２５記載の情報共有システム。

【請求項２８】　上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項２４、２５、２６または２７記載の情報共有システム。

【請求項２９】　取得した暗号化に利用したアルゴリズムを特定する情報をもとに、復号化のアルゴリズムを特定する手段を有する請求項２８記載の情報共有システム。

【請求項３０】　情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程とを少なくとも有する暗号化方法。

【請求項３１】　上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程をさらに有する請求項３０記載の暗号化方法。

【請求項３２】　上記付加情報は、暗号鍵のメッセージダイジェストである請求項３０または３１記載の暗号化方法。

【請求項３３】　上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ＩＤ、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項３０または３１記載の暗号化方法。

【請求項３４】　上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項３０、３１、３２または３３記載の暗号化方法。

【請求項３５】　複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化方法であって、

上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、

上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、

選択した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とを有する復号化方法。

【請求項３６】　複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化方法であって、

上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、

選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、

取得した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とを有する復号化方法。

【請求項３７】　上記付加情報は、暗号鍵のメッセージダイジェストである請求項３５または３７記載の復号化方法。

【請求項３８】　上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ＩＤ、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項３５または３６記載の復号化方法。

【請求項３９】　上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項３５、３６、３７または３８記載の復号化方法。

【請求項４０】　取得した暗号化に利用したアルゴリズムを特定する情報をもとに、復号化のアルゴリズムを特定する工程を有する請求項３９記載の復号化方法。

【請求項４１】　情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特

定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、
上記保管されている複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とを備えた情報処理方法。

【請求項４２】　情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、
上記保管されている付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とを備えた情報処理方法。

【請求項４３】　上記付加情報は、暗号鍵のメッセージダイジェストである請求項４１または４２記載の情報処理方法。

【請求項４４】　上記付加情報は、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ＩＤ、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報である請求項４１または４２記載の情報処理方法。

【請求項４５】　上記付加情報は、暗号化に利用したアルゴリズムを特定するための情報を含む請求項４１、４２、４３または４４記載の情報処理方法。

【請求項４６】　取得した暗号化に利用したアルゴリズムを特定する情報をもとに、復号化のアルゴリズムを特定する工程を有する請求項４５記載の情報処理方法。

【請求項４７】　情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程とをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項４８】　複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、
複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、
選択した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項４９】　いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報に基づいて複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、
選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、
取得した暗号鍵に基づき暗号化情報を復号化して元の情報を取得する工程とをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項５０】　情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、
上記保管されている複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項５１】　情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、
上記保管されている付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とをコン

ピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数のユーザ間での情報共有を目的とし、情報の覗き見や改竄を防ぐための暗号化装置、復号化装置、および情報共有システム、並びに、暗号化方法、復号化方法、情報処理方法、並びに記録媒体に関するものである。

【０００２】

【従来の技術】近年のコンピュータ・ネットワーク技術の発展に伴い、様々なデジタル情報がコンピュータネットワーク上で利用されるようになった。しかし、これらのデジタル情報は、コンピュータ上や、ネットワーク上では、他人の覗き見や改竄が容易である。そこで、特に秘匿の必要があるユーザのプライベート情報やビジネス情報などは、暗号化技術を利用して暗号化した後、取得、伝達、加工、記録する必要がある。

【０００３】このような秘匿する必要のある情報を暗号化するために、データ暗号規格（ＤＥＳ；Data Encryption Standard）などの共通鍵暗号方式が開発された。この方式では、データを暗号化する暗号鍵をユーザ間で共有するため、他のユーザに暗号鍵が取得されないように、配送、記録する必要があった。そのため、この暗号鍵を覗き見や改竄、取得されないようにするために、暗号鍵を別の鍵でさらに暗号化した状態の鍵である暗号化鍵として配送する手段が提案されている。

【０００４】ある情報を共有したい複数のユーザがいる場合に、上記の手法で情報を暗号化するには、これらの暗号鍵や暗号鍵を暗号化するための鍵を管理する鍵管理システムや、情報を共有するユーザをグループ化して管理するグループ管理サーバ、情報へのアクセス制御手段などを利用する必要がある。

【０００５】

【発明が解決しようとする課題】ところで、共有したい秘匿情報毎に、情報を見てもよいユーザは異なる。しかしながら、たとえば、イントラネット上で、鍵管理システムやグループ管理サーバが構築されていたとしても、イントラネットにアクセス権限のない商談中の相手などと、秘匿情報を共有したい場合には、上述した手法では解決できない。

【０００６】すなわち、上述した従来技術では、鍵管理システムや、グループ管理サーバー、アクセス制御手段などを利用しなければ、秘匿データを特定ユーザのみで、共有できないことから、インターネットなどの不特定多数のユーザがアクセスできるネットワーク上などでは、上記のようなシステムや手段を利用せずに、情報を共有できる環境を実現する必要がある。

【０００７】本発明は、かかる事情に鑑みてなされたものであり、その目的は、鍵管理システムや、グループ管理サーバー、アクセス制御手段などを利用しなくても、秘匿情報の複数ユーザによる共有が可能で、また、暗号化情報を保管するデータベースや、サーバ、ファイルシステム等の管理者に情報の内容を見られること防止できる暗号化装置、復号化装置、および情報共有システム、並びに、暗号化方法、復号化方法、情報処理方法、並びに記録媒体を提供することにある。

【０００８】

【課題を解決するための手段】上記目的を達成するため、本発明の暗号化装置は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段とを有する。

【０００９】また、本発明の暗号化装置は、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段を有する。

【００１０】また、本発明の暗号化装置は、上記複数の暗号化鍵および暗号化情報を転送する転送手段、または、上記複数の暗号化鍵、暗号化情報、および付加情報を転送する転送手段を有する。

【００１１】また、本発明は、複数の暗号化鍵および暗号化情報を受けて元の情報を復号する復号化装置であって、上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号鍵に基づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する。

【００１２】また、本発明は、複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化装置であって、上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する暗号鍵取得手段と、上記付加情報に基づいて上記暗号鍵取得手段で取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号鍵に基づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する。

【００１３】また、本発明は、複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化装置であって、上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号鍵に基

づき上記暗号化情報を復号して元の情報を取得する復号化手段とを有する。

【００１４】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えている。

【００１５】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記情報保管装置に保管されている付加情報を取得して当該付加情報に基づき上記暗号鍵取得手段で取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えている。

【００１６】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置と、上記情報保管装置に保管されている上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号鍵に基づき上記情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置とを備えている。

【００１７】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された所定の暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置にうち、少なくとも暗号化装置を備えた第１の装置と、上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第２の装置とを有する。

【００１８】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号鍵取得手段と、上記情報保管装置に保管されている付加情報を取得して当該付加情報に基づき上記暗号鍵取得手段で取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択手段と、上記暗号鍵選択手段で選択された暗号鍵に基づき情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置のうち、少なくとも暗号化装置を備えた第１の装

置と、上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第２の装置とを有する。

【００１９】また、本発明の情報共有システムは、複数のユーザでアクセス可能な情報保管装置と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化手段と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成手段と、上記暗号化鍵生成手段で生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成手段と、上記複数の暗号化鍵、暗号化情報、および付加情報を上記情報保管装置に転送し保管させる転送手段とを有する暗号化装置、および上記情報保管装置に保管されている上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択手段と、上記暗号化鍵選択手段で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得手段と、上記暗号鍵取得手段で取得された暗号鍵に基づき上記情報保管装置に取得した複数の暗号化鍵および付加情報とともに保管されている上記暗号化情報を復号して元の情報を取得する復号化手段とを有する復号化装置のうち、少なくとも暗号化装置を備えた第１の装置と、上記暗号化装置および復号化装置のうち、少なくとも復号化装置を備えた第２の装置とを有する。

【００２０】また、本発明の暗号化方法は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程とを有する。

【００２１】また、本発明の暗号化方法は、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程をさらに有する。

【００２２】また、本発明は、複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化方法であって、上記複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とを有する。

【００２３】また、本発明は、複数の暗号化鍵、暗号化情報、および当該複数の暗号化鍵がいずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を受けて元の情報を復号する復号化方法であって、上記付加情報に基づいて上記複数の暗号化鍵のうちからユーザ

の秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とを有する。

【００２４】また、本発明の情報処理方法は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、上記保管されている複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とを備えている。

【００２５】また、本発明の情報処理方法は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、上記保管されている付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とを備えている。

【００２６】また、本発明の記録媒体は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程とをコンピュータに実行させるプログラムが記録されている。

【００２７】また、本発明の記録媒体は、複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な

暗号鍵を選択する工程と、選択した暗号鍵に基づき上記暗号化情報を復号化して元の情報を取得する工程とをコンピュータに実行させるプログラムが記録されている。

【００２８】また、本発明の記録媒体は、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報に基づいて複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき暗号化情報を復号化して元の情報を取得する工程とをコンピュータに実行させるプログラムが記録されている。

【００２９】また、本発明の記録媒体は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、上記保管されている複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とをコンピュータに実行させるプログラムが記録されている。

【００３０】また、本発明の記録媒体は、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、上記保管されている付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とをコンピュータに実行させるプログラムが記録されている。

【００３１】本発明の暗号化系によれば、複数ユーザが共有したい情報を秘匿しておくために、たとえば共有鍵暗号方式と公開鍵暗号方式が併用される。入力情報は、共有鍵暗号方式で、暗号鍵を用いて暗号化される。次に、情報を共有する複数ユーザ各々の固有の公開鍵が、

取得もしくは、生成される。この複数の公開鍵各々で、暗号鍵が暗号化され、複数の暗号化鍵が生成される。これら暗号化鍵のうち一つは、あるユーザがこの情報を復号化するときに、そのユーザの秘密鍵を用いて復号化することによって、暗号鍵を作成することができる暗号化鍵である。これら複数の暗号化鍵と暗号化情報の両方が、複数ユーザで共有できる場所に転送される。

【００３２】また、本発明に復号化系よれば、複数の暗号化鍵と暗号化情報を取得する手段を備えている。そして、取得した複数の暗号化鍵がユーザ固有の秘密鍵で復号化される。これにより得られた暗号鍵を利用して、暗号化情報が復号化されて、ユーザは、もとの情報を得ることができる。

【００３３】さらに、本発明では、復号化時に取得した複数の暗号化鍵のうち、どの暗号化鍵がユーザの公開鍵で暗号化されたものかを特定するために、付加情報が添付される。この付加情報としては、暗号化系によって作成された、ユーザに関する情報や、暗号鍵に関する情報、暗号化鍵の順番に関する情報、もしくは、それらの情報を暗号化した情報や、それらの情報をもとにハッシュ関数などで作成されたメッセージダイジェストなどが利用される。また、付加情報は、複数の暗号化鍵や暗号化情報と共に複数ユーザで共有できる転送される。この付加情報を受け取った復号化系は、その内容をもとに、どの暗号化鍵をユーザの秘密鍵で復号化すれば、暗号鍵を得られるのかがわかる。以上の２種の暗号化系および復号化系を利用することにより、複数のユーザのみで、情報を共有することができる。

【００３４】また、本発明によれば、以上で説明した暗号化系と復号化系を利用した、ネットワーク上、または、単一装置（端末）上での情報共有システムが実現される。このシステムでは、上述したような暗号化系を組み込んだ端末を利用して、情報が暗号化される。ユーザは、情報を見てもよいユーザの公開鍵を特定することにより、共有するユーザを指定することができる。暗号化後、ネットワークを介して接続されているデータベースや、ファイルシステム、サーバーなどの情報保管装置に、暗号化情報、暗号化鍵、付加情報を転送し、保管される。また、上述した復号化系を組み込んだ装置を利用して、暗号化情報、暗号化鍵、付加情報が取得されて、暗号化情報が復号化されて、もとの情報を得ることができる。この情報の復号化時に、復号化しようとするユーザの公開鍵で暗号化された暗号化鍵がなければ、暗号鍵を生成できないので、第三者の覗き見、改竄を防ぐことができる。この情報共有システムでは、鍵管理システムやグループ管理サーバ、アクセス制御手段などを持たなくても、ユーザが利用する端末に、暗号化系や復号化系を組み込むだけで、情報を共有できるという利点がある。

【００３５】また、現在、様々な共有鍵暗号方式、様々

な公開鍵暗号方式が提案されているが、本発明の暗号化系、復号化系では、様々な方式を利用することができる。そのため、様々な暗号方式の中でもどの方式を利用したのかを明確にする必要がある。本発明は、暗号化系で利用した暗号方式に関する情報（暗号方式情報）を、暗号化情報、暗号化鍵、付加情報と共に転送して、記憶装置に保管される。そして、復号化系では、暗号方式情報をもとに、復号化するための暗号方式が決定される。また、暗号化系と復号化系を組み込んだ一台以上の端末があれば、情報共有システムが実現できる。暗号化系を用いて上記の手順で情報を暗号化し、端末の記録装置に暗号化情報、暗号化鍵、付加情報を記録しておく。この端末を利用する別のユーザは、端末の記憶装置より暗号化情報、暗号化鍵、付加情報を取得し、復号化系を利用して、情報を得ることができる。この暗号化系、復号化系を利用すれば、鍵管理システムやグループ管理サーバ、アクセス制御手段を持たないパーソナルコンピュータなどでも、秘匿情報の複数ユーザによる共有が可能となる。

【００３６】

【発明の実施の形態】以下、本発明の実施形態を図面に関連付けて詳細に説明する。本実施形態では、本発明に係る暗号化装置および復号化装置のいずれか、または、両方が組み込まれた一台以上の端末と、暗号化情報、暗号化鍵、付加情報を格納するデータベース、もしくは、ファイルシステム、サーバーがネットワークに接続された情報共有システム、および、本発明に係る暗号化装置および復号化装置にいずれか、または、両方が組み込まれた一台以上のネットワークに接続された端末で、そのうち一台以上の端末に暗号化情報、暗号化鍵、付加情報を格納できる機能が組み込まれている情報共有システムについて、順を追って説明する。

【００３７】第１実施形態

図１は本発明に係る情報共有システムの基本的な構成図、図２は本発明に係る暗号化装置の構成例を示すブロック図、図３は本発明に係る復号化装置の構成例を示すブロック図である。

【００３８】本実施形態に係る情報共有システムは、図１に示すように、図２に示す暗号化装置１０が組み込まれた第１の端末装置１、図３に示す復号化装置２０が組み込まれた第２の端末装置２、並びに暗号化装置１０で生成された複数の暗号化鍵、暗号化情報、および付加情報を保管するためのWWWサーバ３が、ネットワーク（たとえば、インターネット）４で接続されて構成されている。

【００３９】第１の端末装置１に設けられた暗号化装置１０は、暗号化部１１、暗号鍵生成部１２、記憶部１３、暗号化鍵生成部１４、付加情報生成部１５、並びに転送部１６により構成されている。

【００４０】暗号化部１１は、情報を暗号化するための暗号鍵ｄｋを用いて、たとえば共有鍵暗号方式（たとえばＤＥＳ）により入力情報Ｍを暗号化して暗号化情報Ｍ’を生成し、生成した暗号化情報Ｍ’を転送部１６に出力する。

【００４１】暗号鍵生成部１２は、たとえば乱数発生回路等により構成され、情報を暗号化するための暗号鍵ｄｋを生成し、暗号化部１１および暗号化鍵生成部１４に出力する。なお、暗号鍵ｄｋは、たとえば６４ビットデータとして生成される。

【００４２】なお、この暗号鍵ｄｋを用いた情報の暗号化の一例のフローチャートを、図４に示す。

【００４３】記憶部１３は、たとえばハードディスクにより構成され、本システムを共有する複数ｎのユーザ各々の固有の公開鍵ＰＫ１，ＰＫ２，…，ＰＫｎがあらかじめ記録されており、暗号化鍵生成部１４によりアクセスされる。

【００４４】暗号化鍵生成部１４は、暗号化に用いた暗号鍵ｄｋを、情報Ｍを記憶部１３に記録されているユーザの公開鍵を用い、たとえば公開鍵暗号方式（たとえばＲＳＡ）に基づいて暗号化し、複数の暗号化鍵ＥＫ１，ＥＫ２，…，ＥＫｎを生成し、生成した複数の暗号化鍵ＥＫ１，ＥＫ２，…，ＥＫｎを転送部１６に出力する。この暗号化鍵生成部１４における、暗号鍵ｄｋを公開鍵で暗号化し、複数の暗号化鍵を生成する動作のフローチャートを、図５に示す。

【００４５】付加情報生成部１５は、たとえば暗号鍵ｄｋのメッセージダイジェストｋｍｄをハッシュ関数などで生成し、付加情報ａｊｆとして転送部１６に出力する。なお、付加情報としては、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ＩＤ、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報であってもよい。この付加情報を生成する動作のフローチャートを、図６に示す。

【００４６】転送部１６は、入力情報Ｍの暗号化に伴って生成された複数の暗号化鍵ＥＫ１，ＥＫ２，…，ＥＫｎ、暗号化情報Ｍ’、および付加情報ａｊｆをネットワーク４を介して保管手段装置としてのWWWサーバ３に転送する。

【００４７】なお、暗号化装置１０における上述した情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、上記情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、上記生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、上記各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する、いわゆる暗号化処理工程を実行するためのプログラムは、第１の端末装置（コンピュータ）１で読み出し可

能な記録媒体、たとえば暗号化装置１０やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等に記録され、第１の端末装置１で読み出されて実行される。

【００４８】WWWサーバ３は、暗号化装置１０から転送された入力情報Mの暗号化に伴って生成された複数の暗号化鍵ＥＫ１，ＥＫ２，…，ＥＫｎ、暗号化情報M'、および付加情報ａｊｆを受けて所定の記憶部に記録し、保管する。また、WWWサーバ３には、さらに、今回利用した共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報ｄｅｓｒｓａ（たとえば、ＤＥＳとＲＳＡで暗号化した、など）や、暗号化アルゴリズムの実行に必要な上記以外の情報ｉｎｆｏ（たとえば、ＤＥＳに利用した初期化乱数など）も、一緒に保管されている。

【００４９】第２の端末装置２に設けられた復号化装置２０は、図３に示すように、暗号鍵取得手段としての暗号化鍵復号化部２１、暗号鍵選択部２２、および情報復号化部２３により構成されている。

【００５０】暗号化鍵復号化部２１は、WWWサーバ３に保管されている複数の暗号化鍵を取得し、公開鍵暗号方式（たとえば、ＲＳＡ）を用いてユーザの秘密鍵ｐｖｋで複数の暗号化鍵を復号して暗号鍵を取得し、暗号鍵選択部２２に出力する。実際には、復号化された結果は、一つが所望の暗号鍵で残りは乱数である。なお、この複数の暗号化鍵の復号化動作のフローチャートを図７に示す。

【００５１】暗号鍵選択部２２は、WWWサーバ３に保管されている付加情報を取得し、この付加情報に基づいて、暗号化鍵復号化部２１で取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択して情報復号化部２３に出力する。

【００５２】この暗号鍵選択部２２における暗号鍵の選択動作の具体例のフローチャートを図８に示す。暗号鍵選択部２２は、図８に示すように、暗号化鍵復号化部２１で取得された複数の暗号鍵を取得する（Ｓ２２１）とともに、WWWサーバ３に保管されている付加情報を取得する（Ｓ２２２）。そして、取得した付加情報より、複数の復号化された暗号化鍵の中に暗号鍵が含まれている否か判断する（Ｓ２２３，Ｓ２２４）。ステップＳ２２４において、複数の復号化された暗号化鍵の中に暗号鍵が含まれていると判断した場合には、復号化に利用する暗号鍵を決定し情報復号化部２３に出力する（Ｓ２２５，Ｓ２２６）。一方、ステップＳ２２４において、複数の復号化された暗号化鍵の中に暗号鍵が含まれていないと判断した場合には、ユーザに復号化する権限がないものとして処理を中止する（Ｓ２２７）。

【００５３】情報復号化部２３は、WWWサーバ３に保管されている暗号化情報を取得し、暗号鍵選択部２２で選択された暗号鍵に基づき暗号化情報を復号して元の情報を取得する。この情報復号化部２３の情報復号化動作のフローチャートを図９に示す。

【００５４】なお、復号化装置２０は、WWWサーバ３に複数の暗号化鍵、付加情報、および暗号化情報に加えて保管されている共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報ｄｅｓｒｓａ（たとえば、ＤＥＳとＲＳＡで暗号化した、など）や、暗号化アルゴリズムの実行に必要な上記以外の情報ｉｎｆｏ（たとえば、ＤＥＳに利用した初期化乱数など）も、取得する。そして、たとえば、アルゴリズム識別情報ｄｅｓｒｓａ、情報ｉｎｆｏに基づいて、復号化に利用できるように、アルゴリズムを初期化する。

【００５５】また、復号化装置２０における上述した上記保管されている複数の暗号化鍵からユーザの秘密鍵で暗号化鍵を復号し、暗号鍵を取得する工程と、上記付加情報に基づいて取得した複数の暗号鍵から情報の復号に必要な暗号鍵を選択する工程と、選択した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する、いわゆる復号化処理工程とを実行するためのプログラムは、第２の端末装置（コンピュータ）２で読み出し可能な記録媒体、たとえば復号化装置２０やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等に記録され、第２の端末装置２で読み出されて実行される。

【００５６】次に、上記構成による動作を説明する。なお、ここでは、第１の端末装置１を利用しているユーザＡは、他の２人のユーザ（Ｂ、Ｃ、）と計３人で、情報Mを共有したいと思っている場合を例に説明する。この場合、共有した秘匿情報Mを「こんにちは」、暗号鍵を６４ビットのデータ「１２３４５６７８」、ユーザＡの公開鍵を５１２ビットのデータ「Ａｐｕｂｌｉｃ．．．」、ユーザＢの公開鍵を５１２ビットのデータ「Ｂｐｕｂｌｉｃ．．．」、ユーザＣの公開鍵を５１２ビットのデータ「Ｃｐｕｂｌｉｃ．．．」、並びにユーザＣの秘密鍵を５１２ビットのデータ「Ｃｐｒｉｖａｔｅ．．．」とする。

【００５７】まず、第１の端末装置１の暗号化装置１０では、記録媒体に記録されている暗号化プログラムが読み出されて、以下の処理が実行される。すなわち、入力情報M（「こんにちは」）が暗号化装置１０の暗号化部１１に入力される。このとき、暗号鍵生成部１２で、６４ビットデータである暗号鍵ｄｋ（「１２３４５６７８」）が生成され、この暗号鍵ｄｋが暗号化部１２および暗号化鍵生成部１４に供給される。

【００５８】暗号化部１１では、入力情報Mが共有鍵暗号方式ＤＥＳに基づいて暗号鍵ｄｋを用いて暗号化され、暗号化情報M'（たとえば「＃＄ＴＡ０ｘ！”ｈ」）が生成されて転送部１６に出力される。

【００５９】ここで、暗号化装置１０においては、暗号

化プログラムに基づいて、ユーザAに、誰と情報Mを共有したいのかを、尋ねられる。これに対して、ユーザAは、ユーザB、Cを図示しない入力部（たとえばキーボード）から入力する。この入力を受けて、暗号化装置１０における暗号鍵生成部１４によって、ユーザA、B、Cの公開鍵暗号方式（たとえば、ＲＳＡ）に基づいた公開鍵ＰＫ１（「Ａｐｕｂｌｉｃ．．．」）、ＰＫ２（「Ｂｐｕｂｌｉｃ．．．」）、ＰＫ３（「Ｃｐｕｂｌｉｃ．．．」）が記憶部１３から読み出される。そして、暗号鍵生成部１４において、これらそれぞれの公開鍵を利用して、公開鍵暗号方式に基づいて暗号鍵ｄｋが暗号化され、暗号化鍵ＥＫ１（「Ａｄｆｊｉｎｍｅ」）、ＥＫ２（「Ｚｘｃｕｑｗｅｚ」）、ＥＫ３（「Ｐｑｕｅｉｖｎｍ」）が得られ、転送部１６に出力される。

【００６０】さらに、暗号化装置１０の付加情報生成部１５において、復号化時の暗号鍵ｄｋを特定するための付加情報ａｊｆ（「’＃Ｎｖｌａｍ&」）、具体的には暗号鍵ｄｋのメッセージダイジェストが作成され、転送部１６に出力される。

【００６１】そして、転送部１６により、暗号化情報M’（「＃＄ＴＡ０ｘ！”ｈ」）、暗号化鍵ＥＫ１（「Ａｄｆｊｉｎｍｅ」）、ＥＫ２（「Ｚｘｃｕｑｗｅｚ」）、ＥＫ３（「Ｐｑｕｅｉｖｎｍ」）、付加情報ａｊｆ（「’＃Ｎｖｌａｍ&」を含んだデータがネットワーク４を介してWWWサーバ３に転送され、たとえば図１０に示すように所定の場所に保管される。また、WWWサーバ３には、今回利用した共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報ｄｅｓｒｓａ（たとえば、ＤＥＳとＲＳＡで暗号化した、など）や、暗号化アルゴリズムの実行に必要な上記以外の情報ｉｎｆｏ（たとえば、ＤＥＳに利用した初期化乱数など）も、一緒に保管されている。

【００６２】次に、ユーザCが、Aの作成した情報Mを取得する場合を例に説明する。ユーザCは、まず、復号化装置２０が組み込まれた第２の端末装置２を利用して、WWWサーバ３にアクセスし、暗号化情報M’（「＃＄ＴＡ０ｘ！”ｈ」）、暗号化鍵ＥＫ１（「Ａｄｆｊｉｎｍｅ」）、ＥＫ２（「Ｚｘｃｕｑｗｅｚ」）、ＥＫ３（「Ｐｑｕｅｉｖｎｍ」）、付加情報ａｊｆ（「’＃Ｎｖｌａｍ&」、メッセージダイジェストｋｍｄ）、アルゴリズム識別情報ｄｅｓｒｓａ、情報ｉｎｆｏを取得する。

【００６３】復号化装置２０では、まず、アルゴリズム識別情報ｄｅｓｒｓａ、情報ｉｎｆｏに基づいて、復号化に利用できるように、アルゴリズムが初期化される。そして、暗号化鍵復号化部２１において、まず、暗号化鍵ＥＫ１（「Ａｄｆｊｉｎｍｅ」）、ＥＫ２（「Ｚｘｃｕｑｗｅｚ」）、ＥＫ３（「Ｐｑｕｅｉｖｎｍ」）が、ユーザCの秘密鍵ｐｖｋＣ（「Ｃｐｒｉｖａｔｅ．．．」）で、公開鍵暗号方式（たとえば、ＲＳＡ）を用いて、復号化される。この場合、暗号化鍵ＥＫ１（「Ａｄｆｊｉｎｍｅ」）、ＥＫ２（「Ｚｘｃｕｑｗｅｚ」）は、秘密鍵ｐｖｋＣ（「Ｃｐｒｉｖａｔｅ．．．」）で復号化しても、意味をもたない乱数ｒｎＡ（たとえば乱数「００９８７２３２」）、ｒｎＢ（たとえば乱数「５０２８３７４０」）になるが、暗号化鍵ＥＫ３（「Ｐｑｕｅｉｖｎｍ」）は、暗号鍵ｄｋ（「１２３４５６７８」）に変換される。

【００６４】ここで、乱数２つと、暗号鍵ｄｋが得られたが、実際には、３つとも、ビット列の形式をとるので、どれが、暗号鍵として用いることができるのか、分からない。そこで、復号化装置２０の暗号鍵選択部２２で、付加情報ａｊｆ（「’＃Ｎｖｌａｍ&」）を用いて、３つのビット列のうち、どれが、暗号鍵なのかを選択されて、暗号鍵が特定される。この場合には、乱数ｒｎＡ、ｒｎＢ、暗号鍵ｄｋのメッセージダイジェストが付加情報として生成されており（たとえば、ＭＤ５などを利用して）、それらのうち、WWWサーバ３より取得したメッセージダイジェストｋｍｄと一致するメッセージダイジェストが生成したビット列（この場合は、ｄｋ）が、暗号鍵として、選択される。

【００６５】本例の場合、乱数「００９８７２３２」、乱数「５０２８３７４０」、暗号鍵「１２３４５６７８」のメッセージダイジェストが作成され、それぞれｍｅｓ１「ｈｉｎｅ@ｈａｎ」、ｍｅｓ２「ｕｉｎｅｂ’&ｖ」、ｍｅｓ３「’＃Ｎｖｌａｍ&」である場合には、ｍｓｅ３が付加情報として等しいことから、３つ目の「１２３４５６７８」が暗号鍵として特定できる。

【００６６】そして、情報復号化部２３において、選択された暗号鍵ｄｋ（「１２３４５６７８」）を利用することによって、暗号化情報M’（「＃＄ＴＡ０ｘ！”ｈ」）が共有鍵暗号方式（たとえば、ＤＥＳ）を用いて復号化されて、もとの情報M（「こんにちは」）が得られる。

【００６７】以上説明したように、本第１の実施形態によれば、複数のユーザでアクセス可能なWWWサーバ３と、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する暗号化部１１と、暗号化に用いた暗号鍵を、情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する暗号化鍵生成部１４と、生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する付加情報生成部１５と、複数の暗号化鍵、暗号化情報、および付加情報をWWWサーバ３に転送し保管させる転送部１６とを有する暗号化装置１０を備えた第１の端末装置１と、保管されている複数の暗号化鍵を取得してユーザの秘密鍵で当該暗号化鍵を復号して暗号鍵を取得する暗号化鍵復号化部２１と、保管されている付加情報を取得して当該付加情報に

基づき取得された複数の暗号鍵から情報の復号に必要な暗号鍵を選択する暗号鍵選択部２２と、選択された暗号鍵に基づき保管されている暗号化情報を復号して元の情報を取得する情報復号化部２３とを有する復号化装置２０を備えた第２の端末装置２とを設け、これらをネットワーク４で接続したので、情報の復号化時に、復号化しようとするユーザの公開鍵で暗号化された暗号化鍵がなければ、暗号鍵を生成できないので、第三者の覗き見、改竄を防ぐことができる。この情報共有システムでは、鍵管理システムやグループ管理サーバ、アクセス制御手段などを持たなくても、ユーザが利用する端末に、暗号化系や復号化系を組み込むだけで、情報を共有できるという利点がある。

【００６８】第２実施形態

本第２の実施形態では、暗号化装置１０が組み込まれた第１の端末装置１、復号化装置２０が組み込まれた第２の端末装置２が、ネットワーク（たとえば、ＬＡＮ）で接続されている場合の例を、以下に説明する。

【００６９】この場合は、WWWサーバは不要であり、その代わりに第１の端末装置１の記憶装置が用いられる。また、第２の端末装置２の復号化装置２０ａは、たとえば図１１に示すように、第１の端末装置１の記憶装置に保管されている付加情報に基づいて複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する暗号化鍵選択部２４と、暗号化鍵選択部で選択された暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する暗号鍵取得部２５と、暗号鍵取得部２５で取得された暗号鍵に基づき取得した複数の暗号化鍵および付加情報とともに保管されている暗号化情報を復号して元の情報を取得する情報復号化部２６とを有するように構成される。なお、図３に示す復号化装置が本第２の実施形態に適用できることはいうまでもない。

【００７０】次に、本第２の実施形態の動作について説明する。ここでは、第１の端末装置１を利用しているユーザＡは、他の３人のユーザ（Ｂ、Ｃ、Ｄ）と計４人で、情報Ｍを共有しているものとする。ユーザＡは、暗号化装置１０を利用して、情報Ｍを暗号化して、第１の端末装置１の情報保管機能（たとえば、ハードディスクのファイルシステム）に暗号化情報を保管しておく。

【００７１】まず、第１の端末装置１の暗号化装置１０では、記録媒体に記録されている暗号化プログラムが読み出されて、以下の処理が実行される。すなわち、入力情報Ｍが暗号化装置１０の暗号化部１１に入力される。このとき、暗号鍵生成部１２で、暗号鍵ｄｋが生成され、この暗号鍵ｄｋが暗号化部１２および暗号化鍵生成部１４に供給される。

【００７２】暗号化部１１では、入力情報Ｍが共有鍵暗号方式ＤＥＳに基づいて暗号鍵ｄｋを用いて暗号化され、暗号化情報Ｍ’が生成されて転送部１６に出力される。

【００７３】ここで、暗号化装置１０においては、暗号化プログラムに基づいて、ユーザＡに、誰と情報Ｍを共有したいのかを、尋ねられる。これに対して、ユーザＡは、ユーザＢ、Ｃ、Ｄを図示しない入力部（たとえばキーボード）から入力する。この入力をうけて、暗号化装置１０における暗号鍵生成部１４によって、ユーザＢ、Ｃ、Ｄの公開鍵暗号方式（たとえば、ＲＳＡ）に基づいた公開鍵ＰＫＢ、ＰＫＣ、ＰＫＤが記憶部１３から読み出される。そして、暗号鍵生成部１４において、これらそれぞれの公開鍵を利用して、公開鍵暗号方式に基づいて暗号鍵ｄｋが暗号化され、暗号化鍵ＥＫＢ、ＥＫＣ、ＥＫＤが得られ、転送部１６に出力される。

【００７４】さらに、暗号化装置１０の付加情報生成部１５において、たとえば、暗号化鍵ＥＫＢ、ＥＫＣ、ＥＫＤとユーザＢ、Ｃ、のＩＤ、ｉｄＢ、ｉｄＣ、ｉｄＤを対応づける対応表ｍｔＢＣＤが付加情報として作成される。これらの情報を生成終了すると、転送部１６により暗号化情報Ｍ’、暗号化鍵ＥＫＢ、ＥＫＣ、ＥＫＤ、対応表ｍｔＢＣＤが第１の端末装置１の記憶装置（たとえば、ハードディスク）に保管される。また、第１の端末装置１の記憶装置には、今回利用した共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報ｄｅｓｒｓａ（たとえば、ＤＥＳとＲＳＡで暗号化した、など）や、暗号化アルゴリズムの実行に必要な上記以外の情報ｉｎｆｏ（たとえば、ＤＥＳに利用した初期化乱数など）も、一緒に保管されている。

【００７５】次に、ユーザＣが、Ａの作成した情報Ｍを取得する場合を例に説明する。ユーザＣは、まず、復号化装置２０が組み込まれた第２の端末装置２を利用して、第１の端末装置１の記憶装置をアクセスし、暗号化情報Ｍ’、暗号化鍵ＥＫＢ、ＥＫＣ、ＥＫＤ、付加情報ａｊｆ（対応表ｍｔＢＣＤ）、アルゴリズム識別情報ｄｅｓｒｓａ、情報ｉｎｆｏを取得する。

【００７６】復号化装置２０では、まず、アルゴリズム識別情報ｄｅｓｒｓａ、情報ｉｎｆｏに基づいて、復号化に利用できるように、アルゴリズムが初期化される。ここでは、暗号化鍵ＥＫＢ、ＥＫＣ、ＥＫＤの３つの暗号化鍵が得られたが、実際には、３つとも、ビット列の形式をとるので、どれを復号化して、暗号鍵として用いることができるのか、分からない。そこで、暗号鍵選択部２４で、付加情報（この場合は、対応表ｍｔＢＣＤ）を用いて、３つのビット列のうち、どれが、暗号鍵なのかが選択される。そして、対応表より、暗号化鍵復号部２５において暗号化鍵ＥＫＣがユーザＣの秘密鍵ｐｖｋＣで、公開鍵暗号方式（たとえば、ＲＳＡ）を用いて、復号化され、暗号鍵ｄｋが得られる。

【００７７】そして、情報復号化部２６において、復号化暗号鍵ｄｋを利用することによって、暗号化情報Ｍ’が共有鍵暗号方式（たとえば、ＤＥＳ）を用いて復号化

されて、もとの情報Mが得られる。

【００７８】以上説明したように、本第２の実施形態においても、上述した第１の実施形態の効果と同様の効果を得ることができる。

【００７９】なお、上述した第１および第２の実施形態では、第１の端末装置１には暗号化装置１０のみを設け、第２の端末装置２には暗号化装置２０のみを設けた場合を例に説明したが、これに限定されるものではなく、第１および第２の端末装置１，２に暗号化装置１０および復号化装置２０の両方を組み込むことも可能であり、この場合も上述したと同様の効果を得ることができる。

【００８０】この場合、端末装置１、２においては、情報を暗号化するための暗号鍵を用いて入力情報を暗号化して暗号化情報を生成する工程と、暗号化に用いた暗号鍵を、情報を見てもよい少なくとも一のユーザの公開鍵で暗号化し、複数の暗号化鍵を生成する工程と、生成された複数の暗号化鍵が、いずれのユーザの公開鍵で暗号化されたものであるかを特定する付加情報を生成する工程と、各工程で取得した複数の暗号化鍵、暗号化情報、および付加情報を保管する工程とを有する暗号化処理工程と、保管されている付加情報に基づいて上記複数の暗号化鍵のうちからユーザの秘密鍵で復号化すべき暗号化鍵を選択する工程と、選択した暗号化鍵をユーザの秘密鍵で復号し、暗号鍵を取得する工程と、取得した暗号鍵に基づき上記保管されている暗号化情報を復号化して元の情報を取得する工程とを有する復号化処理工程とをコンピュータに実行させるプログラムが記録媒体、第１および第２の端末装置１，２やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等に記録され、第１および第２の端末装置１で読み出されて実行される。

【００８１】このように両方の端末装置１、２に、復号化系を組み込んでおくと、端末１を利用するユーザDも、端末装置１を使って、上記の方法で、情報Mを得ることができる。また、このように暗号化、復号化の両系を一つの端末に組み込んでおけば、端末装置１だけで、情報共有システムが実現できる利点がある。

【００８２】また、上述した第１および第２の実施形態では、暗号化処理工程および復号化処理工程を実行するためのプログラムが記録され、コンピュータで読み出し可能な記録媒体として、暗号化装置、復号化装置やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等を例に説明したが、

これに限定されるものではなく、他の例として、たとえばインターネットの専用線や電話回線等の通信線路のように、通信プログラムを伝送する際にこの通信プログラムを一定時間保持するデータ伝送路等を挙げることができる。

【００８３】

【発明の効果】以上説明したように、本発明によれば、鍵管理システムや、グループ管理サーバー、アクセス制御手段などを利用しなくても、秘匿情報の複数ユーザによる共有が、可能となる。また、暗号化情報を保管するデータベースや、サーバ、ファイルシステムの管理者に情報の内容を見られてしまう可能性もない。

【図面の簡単な説明】

【図１】本発明に係る情報共有システムの基本的な構成図である。

【図２】本発明に係る暗号化装置の構成例を示すブロック図である。

【図３】本発明に係る復号化装置の構成例を示すブロック図である。

【図４】暗号鍵を用いた情報の暗号化の一例を示すフローチャートである。

【図５】暗号化鍵生成部における、暗号鍵を公開鍵で暗号化し、複数の暗号化鍵を生成する動作を示すフローチャートである。

【図６】付加情報を生成する動作のフローチャートである。

【図７】複数の暗号化鍵の復号化動作を示すフローチャートである。

【図８】暗号鍵選択部における暗号鍵の選択動作の具体例を示すフローチャートである。

【図９】情報復号化部の情報復号化動作を示すフローチャートである。

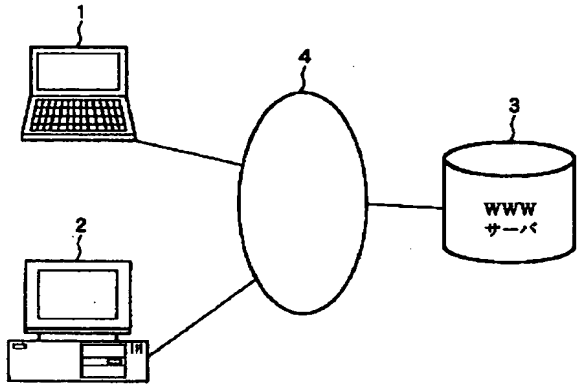
【図１０】WWWサーバに記録されるデータ例を示す図である。

【図１１】本発明に係る復号化装置の他の構成例を示すブロック図である。

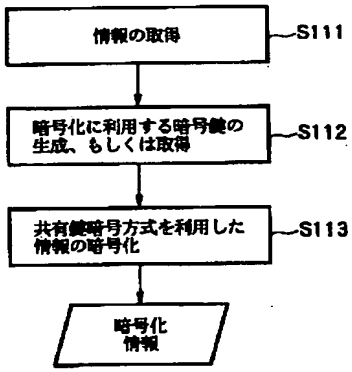
【符号の説明】

１…第１の端末装置、２…第２の端末装置、３…WWWサーバ（情報保管装置）、４…ネットワーク、１０…暗号化装置、１１…暗号化部、１２…暗号鍵生成部、１３…記憶部、１４…暗号化鍵生成部、１５…付加情報生成部、１６…転送部１６、２０…復号化装置、２１，２５…暗号化鍵復号化部、２２…暗号鍵選択部、２３，２６…情報復号化部、２４…暗号化鍵選択部。

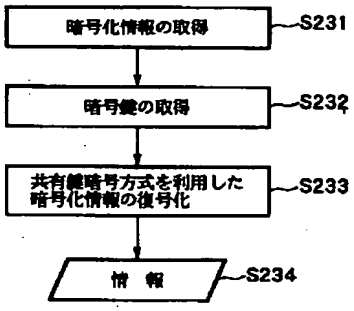
【図１】



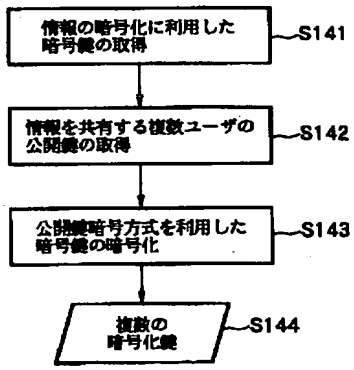
【図４】



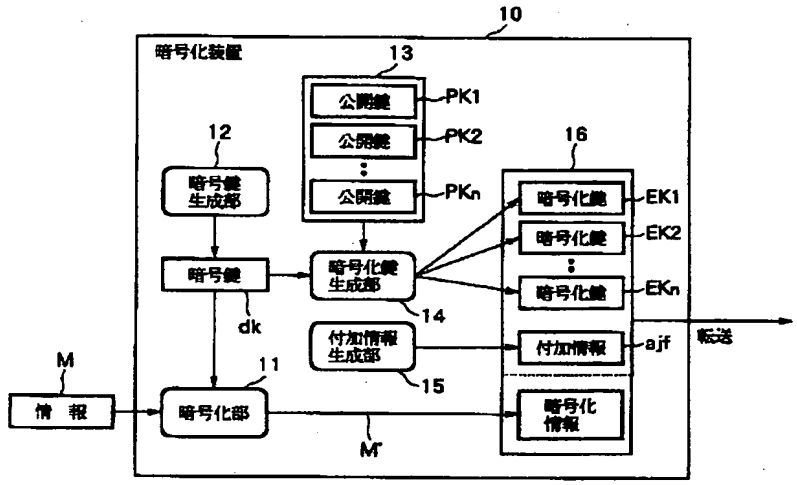
【図９】



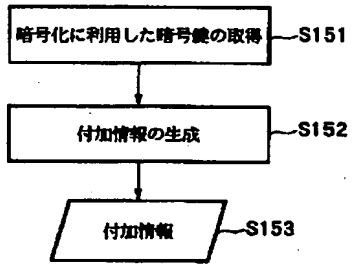
【図５】



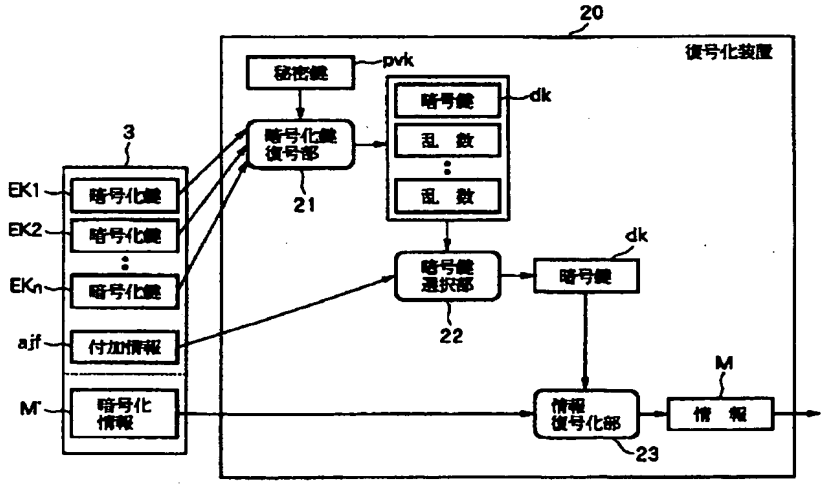
【図２】



【図６】



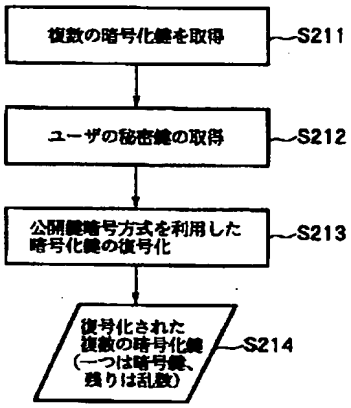
【図３】



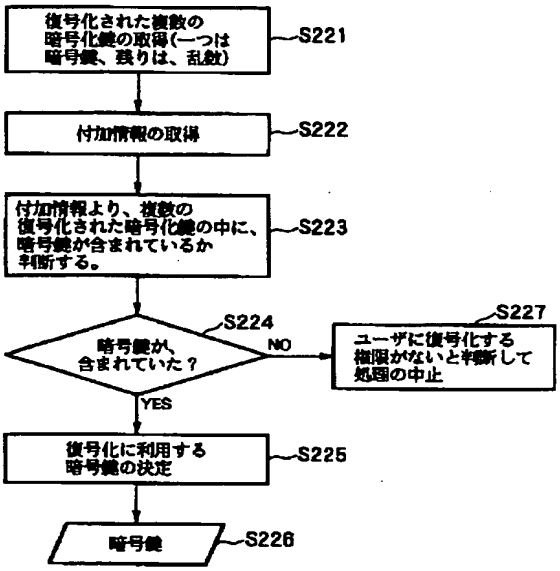
【図１０】

Key	Adfjtnme
Key	Zxcuqwez
Key	Ponelvnm
Info	' # Nvlam &
Content	# $ TA0x ! "h

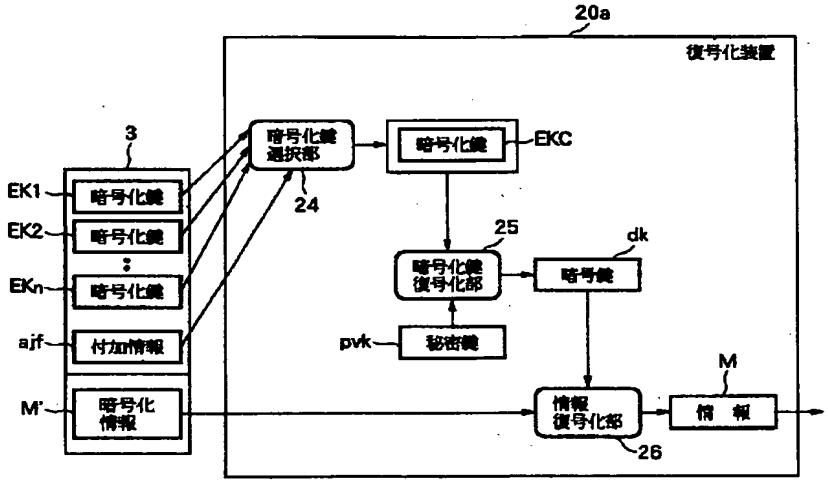
【図７】


複数の暗号化鍵を取得
S211
ユーザの秘密鍵の取得
S212
公開鍵暗号方式を利用した
暗号化鍵の復号化
S213
復号化された
複数の暗号化鍵
(一つは暗号鍵、
残りは乱数)
S214

【図８】


復号化された複数の
暗号化鍵の取得(一つは
暗号鍵、残りは、乱数)
S221
付加情報の取得
S222
付加情報より、複数の
復号化された暗号化鍵の中に、
暗号鍵が含まれているか
判断する。
S223
暗号鍵が、
含まれていた？
S224
NO
ユーザに復号化する
権限がないと判断して
処理の中止
S227
YES
復号化に利用する
暗号鍵の決定
S225
暗号鍵
S226

【図１１】


20a
復号化装置
3
EK1
暗号化鍵
EK2
暗号化鍵
EKn
暗号化鍵
ajf
付加情報
M'
暗号化
情報
暗号化鍵
選択部
24
暗号化鍵
EKC
25
暗号化鍵
復号化部
dk
暗号鍵
pvk
秘密鍵
M
情報
復号化部
情報
26